DoD CYBER
CRIME CENTER

VULNERABILITY DISCLOSURE PROGRAM ANNUAL REPORT 2020

VOLUME 2

MESSAGE FROM THE DC3 EXECUTIVE DIRECTOR

WELCOME to the second VDP Annual Report, 2020 Edition!

I want to personally thank you for taking time out of your busy schedule to read about what the VDP team accomplished over the past year. I feel confident in saying that 2020 was one of the most unique and challenging years we've navigated as an organization, with a wide array of unforeseeable pandemic-related impacts on the DC3 team and the many mission partners with whom we collaborate and support. While difficult to convey all the challenges the DoD VDP team faced, I can tell you they successfully rallied to overcome two concurrent and imposing obstacles.

First, in order to minimize COVID-19 transmission, they had to rapidly migrate from a consolidated office-based operation to a remote and dispersed operation. In addition to deploying multiple FEDRAMP-approved collaboration technologies such as Slack and ZoomGOV, the VDP team rapidly launched the NIPRNet version of the DoD's Vulnerability Report Management Network (VRMN). This protected hundreds of teleworking military, civilians, and contract employees across the DoD by facilitating easier remote access to critical vulnerability data, and by extension, enabling sustained mitigation efforts regardless of their work location.

Second, the VDP team experienced what can only be described as an incredible increase in vulnerability reporting by the security researcher community. In a single year, the VDP team processed 11,984 vulnerability reports, which is nearly the total number of reports received in the 3 previous years COMBINED. To put that in perspective: 2020 was a 299% new report increase as compared to 2019. And as long as the researchers continue to spend more time at home, we believe that this trend will continue.

The team is well-positioned to expeditiously confront any challenge 2021 may bring. They do so knowing that every vulnerability mitigated will harden our Nation's cyber defenses and they are directly supporting the US Warfighter.

V/r,

Jeffery D. Specht, SES, DAF
Executive Director
DoD Cyber Crime Center (DC3)

VDP IN GOVERNMENT

1. NATIONAL CYBER STRATEGY
   - A. PILLAR II: PROMOTE AMERICAN PROSPERITY
     - I. PROMOTE FULL LIFECYCLE CYBERSECURITY
2. IOT CYBERSECURITY IMPROVEMENT ACT OF 2020 (H.R. 1668)
3. OMB MEMORANDUM M-20-32
4. DHS CISA BOD 20-01
5. DODI 8531.01 DOD VULNERABILITY MANAGEMENT

DOD VDP IN THE NEWS

2020 was a very eventful year. Ethical hackers have used a worldwide pandemic to dramatically improve the Department's cyber hygiene level. Sometimes DOD VDP findings make news.

Keep up-to-date on the latest DOD VDP stories at: https://www.dc3.mil/Vulnerability-Disclosure/VDP-Stories/

DIB–VDP PILOT PROGRAM

DEFINING A VULNERABILITY DISCLOSURE PROGRAM

In November 2019, the Department of Defense Cyber Crime Center (DC3) and The Defense Counterintelligence and Security Agency (DCSA) signed a Memorandum of Agreement (MoA) to discover new ways to share information security data. One of the areas of cooperation between the two organizations was to discover how to share vulnerability data with Defense Industrial Base (DIB) companies. At DC3, the Department of Defense's Vulnerability Disclosure Program (DOD VDP) currently shares vulnerability data with internal DoD asset owners via JFHQ-DoDIN, which has primary responsibility for defending DoD's enterprise data systems.

A Vulnerability Disclosure Program (VDP) consists of three top-level components:

- **Policy:** A VDP includes clear guidelines for conducting crowdsourced vulnerability discovery activities within its approved scope of operation.
- **Channel:** A VDP must provide a secure and protected channel for security researchers to report vulnerabilities with the promise of 'safe harbor' from prosecution.
- **Process:** A VDP includes internal processes for triaging, validating, and mitigation of vulnerabilities in an appropriate and timely manner.

The DIB-VDP Pilot Program leverages the lessons learned from the DOD VDP's over 25,000 vulnerability reports; 16,774 of which were triaged, validated, and mitigated within the past four years.

> “THE VDP PROGRAM HAS PROVIDED VALUABLE ADVANCE VULNERABILITY DETECTION FOR FORWARD FACING DOD WEBSITES WHICH HAS RESULTED IN JFHQ-DODIN'S EARLY ENGAGEMENT WITH TERRAIN OWNERS TO REMEDIATE OR MITIGATE VULNERABILITIES PRIOR TO MALICIOUS EXPLOITS.”
>
> —**Mrs. Margaret Mallon**, JFHQ-DODIN Vulnerability Disclosure Program Team Lead

DIB–VDP INDUSTRY DAY FOR 12–MONTH PILOT

Independent analysis by the Software Engineering Institute at Carnegie Melon University of DIB cyber capabilities, shortfalls, and the strength of the DoD VDP during the feasibility study has determined that launching the DIB-VDP pilot can significantly improve the cyber defense, hygiene, and resiliency of companies that do not have the resources to launch this service on their own. Each company will agree to the pilot's terms of service and define which of their systems will be in scope for the crowd-sourced security researchers.

The DIB-VDP will receive reports and forward to the appropriate system owners for mitigation based on severity of the vulnerabilities and risk to their system.

The 12-month DIB-VDP Pilot Program will begin on April 5, 2021 and a DIB-VDP Industry Day was held February 12, 2021 to answer questions and facilitate the on-boarding process.

https://github.com/DC3-VDP/DIB-VDP-Pilot
DIB-VDP@dc3.mil

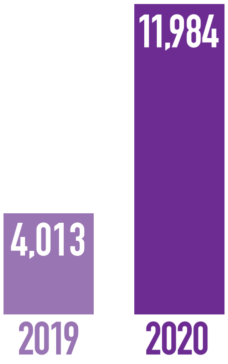
HIGH SPEED – LOW DRAG

KEEPING DOD VDP FLYING HIGH DURING COVID-19

Our team has, without hesitation plunged through the difficulties over this past year. Like every other high performing team, VDP has gone through an array of necessary evolutions to arrive at the team of today. We have come together to achieve unified objectives, leaned in to rely upon individual strengths in order to eliminate team weaknesses and streamlined processes to strip away unnecessary muscle movements. Challenges are being met head on with aggressive determination, and developing strategic solutions have become part of the VDP ethos.

Teleworking, while it has all new gaps and struggles; this opportunity has forged a stronger DoD VDP team and influenced much welcomed growth. COVID-19 operations have increased productivity, researcher program interest, and has accelerated the VDP submissions to surpass almost double the volume in comparison to any previous year. We thank all of our stakeholders and the cyber community for the continued engagement and support.

TOTAL NEW VULNERABILITIES SUBMITTED



THE VDP PROFESSOR

Charles "Chuck" Yarbrough, Software Engineering Institute (SEI) Senior Engineer, served in the DoD Vulnerability Disclosure Program (VDP) developing strategy since 2016. Prior to joining VDP, Chuck supported the DC3 mission space collectively for over a decade. Chuck's thought provoking discussions provided tremendous opportunity for organizational growth. His ideas now lie in the very fabric of the DOD VDP. He brilliantly helped transition the VDP into a self-sustaining operational mission. Chuck analyzed the way ahead, provided ideas for cross-collaboration, facilitated internal and external partnership opportunities. His unwavering ethics, desire "to do good work," laser focus on protecting DoD assets and the war fighter, endures in this organization.

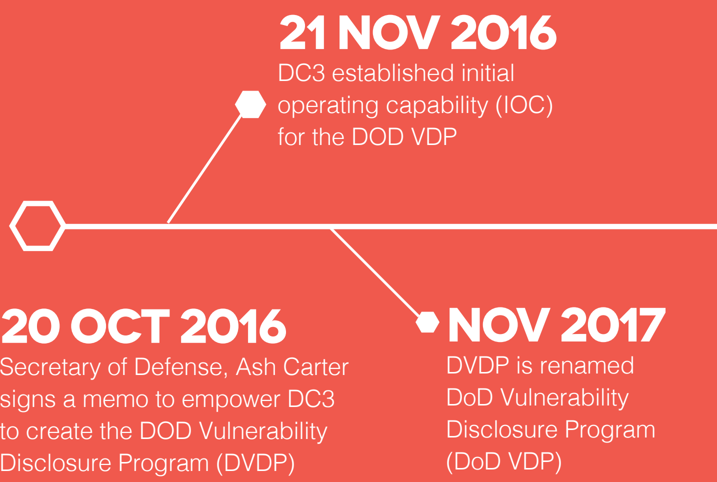
Chuck credits his family with his early lessons of integrity, humility, and stewardship. He is never above helping his fellow teammates or to share his vast knowledge and keen perspective. The VDP team agrees, every member benefited significantly from working with "The VDP Professor." We look forward to what you conquer next.

It has been an honor to serve the VDP mission together.
We wish you all the best on your future endeavors! –VDP Team

HISTORY OF THE DOD VDP

On 20 October 2016, Secretary of Defense, Ash Carter, signed a memo directing DC3 to lead an internal effort to "bring white hat hackers into the fight to the benefit of the DOD" following the success of the Hack the Pentagon bug bounty pilot. Only a month later, on 21 November 2016, the DoD Vulnerability Disclosure Program (DVDP) launched. Mr. Jon Stivers, DVDP Director, established the "One Team, One Jersey" approach to the unification of effort between DC3, US Cyber Command's (USCC) Joint Force Headquarters DoD Information Network (JFHQ-DODIN) and HackerOne's crowd-sourced white hat hacker community. Four years later, DoD VDP is going strong. Mr. Kristopher Johnson, VDP Director, is looking towards the future. The DoD VDP leadership is called upon to provide expert vulnerability disclosure consultation to the White House, Congress, DOD, DOJ, DHS, state governments, 4th estate, academia, cyber committees, private and cleared defense industry.

THE BEGINNING:



21 NOV 2016
DC3 established initial operating capability (IOC) for the DOD VDP

20 OCT 2016
Secretary of Defense, Ash Carter signs a memo to empower DC3 to create the DOD Vulnerability Disclosure Program (DVDP)

NOV 2017
DVDP is renamed DoD Vulnerability Disclosure Program (DoD VDP)

HACKER-POWERED SECURITY

BREAKING RECORDS IN VULNERABILITY REPORTING

25,276
VULNERABILITIES SINCE LAUNCH

2,204
RESEARCHERS SINCE LAUNCH

16,774
ACTIONABLE REPORTS SINCE LAUNCH

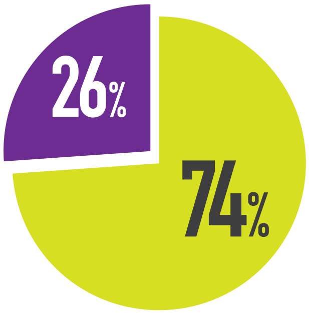
11,984
NEW VULNERABILITIES IN 2020

744
RESEARCHER PARTNERSHIP GROWTH IN 2020 ALONE

7,963
ACTIONABLE REPORTS IN 2020

TOTAL ATTEMPTED MITIGATIONS

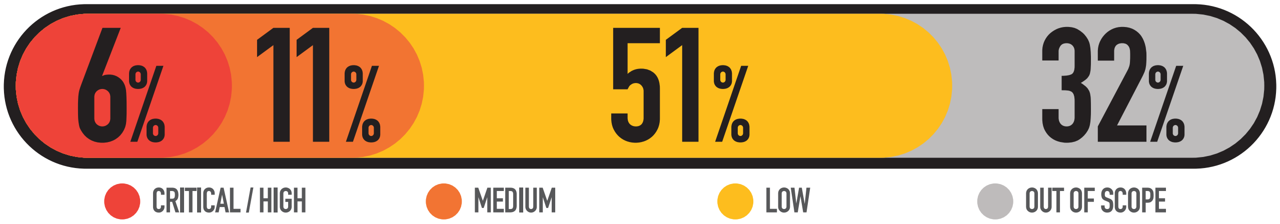
7,995



● 5,999 Successfully Mitigated Reports

● 1,996 Unsuccessful Mitigation Attempts

2020 REPORT SEVERITY RATINGS



RECENT SUCCESSES:

OCT 2018

AMRDEC Safe Access File Exchange (SAFE): Taken offline due to CAC bypass vulnerability

AUG 2019

Pulse Secure VPN: 129 separate critical vulnerabilities reported two days after DEFCON

NOV 2019

Awarded 2019 DOD CIO Team Award for Cybersecurity with a $64M cost-savings from averting cyber-attacks

APR 2020

Federal Voting Assistance Program (FVAP): Discovered 7 critical vulnerabilities that were mitigated to provide election security

JUL 2020

Cisco Adaptive Security Appliance (ASA) and (FTD)

15 SEP 2020

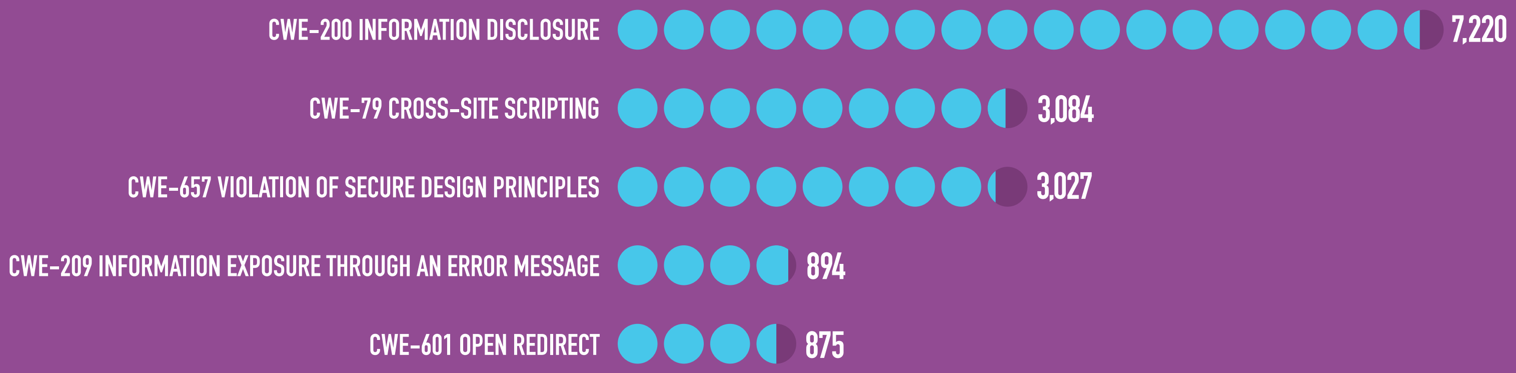
DOD VDP and the Vulnerability Report Management Network (VRMN) are included in the **DOD Instruction 8530.01: DoD Vulnerability Management**

2020 VRMN ANALYTICS

Vulnerability Report Management Network (VRMN) is a JIRA-based platform where the DoD has streamlined every step of the vulnerability mitigation process.

PROTECTING THE 2020 ELECTION

VDP assisted in securing the Federal Voting Assistance Program or FVAP in April 2020. Seven vulnerabilities were discovered on FVAP.gov to include clear text passwords, vulnerable software versions, and various webserver configuration flaws. DOD VDP coordinated weekly with Defense Human Resources Agency (DHRA), OSD, Senator Wyden's Congressional staff, and JFHQ-DODIN until all seven vulnerabilities were successfully mitigated and validated.



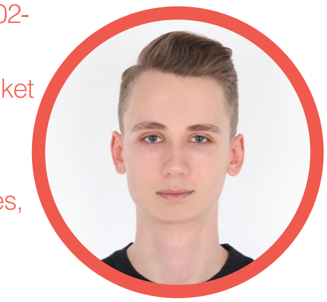
MONERO CRYPTOCURRENCY MINING ON DOD SERVER

The online news site ZDNet wrote an article on February 5th about a DODIN vulnerability discovered by a VDP researcher. In January we processed a report detailing a misconfigured instance of the R&D software Jenkins on a DoD website in an Amazon Web Services (AWS) cloud. Further testing of the website by the VDP team uncovered an unidentified botnet that was actively mining the cryptocurrency Monero. The team quickly worked with JFHQ-DODIN and the system owners to take the compromised server offline until the vulnerability could be mitigated.

https://www.zdnet.com/article/bug-hunter-finds-cryptocurrency-mining-botnet-on-dod-network

2020 VDP RESEARCHER OF THE YEAR

Paolo Arnolfo aka **@sw33tlie** is a frequent contributor in the bug bounty world and made a huge splash in the DoD VDP with his submissions. His esteemed and timely discoveries were instrumental in mitigating Cisco's CVE-2020-3452/3187. Paolo's rolling contributions did not stop there, he also found vulnerabilities on CVE-2019-18935, successful Remote Code Execution (RCE) on numerous IP addresses, and even leakage from an AWS S3 bucket. The DoD is lucky to have contributors with the quality submissions of researchers like him. Although this was a unique year, a lot of researchers stepped up which is evident with each of the "VDP Researcher of the Month" recipients. However, **Sw33tlie** emerged as the overwhelming victor of **Researcher of the Year**. **Paolo @ sw33tlie Arnolfo** burst onto the scene in 2020 by submitting over 150 reports in a 3-month time-span. Over 80% of those submissions were high/critical dealing with Cisco Path Traversal Vulnerabilities (CVE-202-3452/3187), Telerik UI vulnerabilities (CVE-2019-18935), and AWS S3 bucket information leakage. The **2020 VDP Researcher of the Year** also has submissions to a myriad of companies, including Comcast, FireEye, and Overstock. The entire VDP thanks **sw33tlie** for his dedication to our program, and look forward to seeing all his new findings in 2021!



PERFORMANCE STATS 126 1 0

● CRITICAL / HIGH ● MEDIUM ● LOW

> “ **IN DDS, WE HIRE TOP TECHNICAL TALENT, WHICH MEANS BRINGING IN HACKERS TO HELP FIND AND FIX VULNERABILITIES IN DOD SYSTEMS. WE ARE USING MODERN APPROACHES TO LEAPFROG THE CURRENT STATE OF TECHNOLOGY, TRANSFORM GOVERNMENT CULTURE, AND TO MORE RAPIDLY SECURE THE DOD. THE DOD VULNERABILITY DISCLOSURE POLICY IS AN EXAMPLE OF THE VALUE THAT THESE EFFORTS CAN BRING TO GOVERNMENT AND NATIONAL DEFENSE.** ”
>
> —**Brett Goldstein**, Director, Defense Digital Service

CVE-2020-3452 – CISCO ASA AND FTD

VDP experienced a huge spike in July 2020 thanks to the 608 reports submitted in response to CVE-2020-3452. This was the most discovered Common Vulnerabilities and Exposures (CVE) reported to VDP. The second highest single CVE discovery belongs to the Pulse Secure VPN in Aug-Sep 2019 which received 129 reports.

CVE-2020-3452 is a DoDIN-wide vulnerability impacting much of the Department's Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD) Software. If exploited, this CVE could allow an unauthenticated remote attacker to conduct a low complexity directory traversal attack with high impacts to confidentiality via access to sensitive files on the targeted system. Responsive to the volume of discovery and reporting, the VDP team immediately engaged USCYBERCOM and JFHQ-DODIN to ensure appropriate awareness and enable coordinated mitigation efforts.

Additional information specific to this vulnerability can be found at **https://nvd.nist.gov/vuln/detail/CVE-2020-3452**.

VDP

CFL

DCISE

OED

CTA

TSD

DEPARTMENT OF DEFENSE
CYBER CRIME CENTER

> BEFORE VDP, THE DEFENSE DEPARTMENT HAD NO OBVIOUS WAY OF RECEIVING AND MITIGATING VULNERABILITY ISSUES DISCOVERED BY EXTERNAL RESEARCHERS. AS A RESULT, MANY ISSUES WENT UNREPORTED. WITH VDP, THE NATION IS MORE SECURE AND DDS IS GRATEFUL TO THE AMAZING COMMUNITY OF RESEARCHERS WHO HAVE WORKED TO EXPOSE THE VULNERABILITIES AND STRENGTHEN NATIONAL DEFENSE.
>
> —**Alexander "RoRo" Romero**, Digital Service Expert, Defense Digital Service